(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 926 630 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
30.06.1999 Patentblatt 1999/26

(51) Int. Cl.[6]: G07B 17/00, G07B 17/04

(21) Anmeldenummer: 98119851.8

(22) Anmeldetag: 20.10.1998

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: 29.10.1997 DE 19748954

(71) Anmelder:
Francotyp-Postalia AG & Co.
16547 Birkenwerder (DE)

(72) Erfinder:
Pauschinger, Dieter Dr.
16540 Hohen Neuendorf (DE)

(54) Verfahren für eine digital druckende Frankiermaschine zur Erzeugung und Überprüfung eines Sicherheitsabdruckes

(57) Die Erfindung betrifft ein Verfahren für eine digital druckende Frankiermaschine und zur Erzeugung und Überprüfung eines Sicherheitsabdruckes, wobei wesentliche Frankierinformationen zusammen mit einer Signatur auf ein Poststück im maschinenlesbaren Bereich des Frankierbildes aufgedruckt werden. Für den Abdruck, der human lesbar und außerdem sicher maschinenlesbar ist, kann ein Druckkopf üblicher Druckbreite eingesetzt werden, weil durch ein modifiziertes Public Key-Verfahren die zu druckende maschinenlesbare Informationsmenge reduziert ist, weil der geheime Schreibschlüssel Kw und der Algorithmus zur Verschlüsselung auf der Frankiermaschinenseite in einem Sicherheitsgerät PSD gespeichert ist, sowie weil der öffentliche Leseschlüssel und sein Zertifikat der Frankiermaschinen-Kennung zugeordnet einer Datenbank auf der Postseite entnommen werden kann. Das für Frankiermaschinen modifizierte Public Key-Verfahren zeichnet sich durch eine einfache Schlüsselgenerierung und Verschlüsselung der Botschaft auf der Frankiermaschinenseite und eine einfache Entschlüsselung der Botschaft auf der Postseite aus.

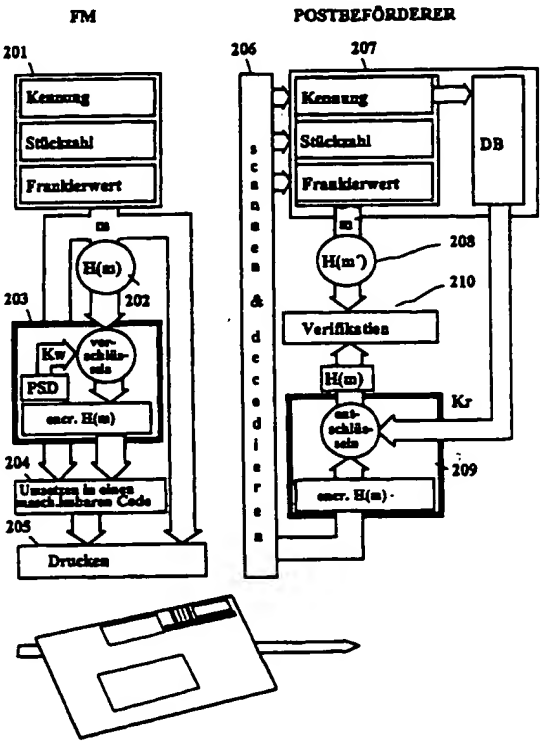

Fig. 2

EP 0 926 630 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren für eine digital druckende Frankiermaschine zur Erzeugung und Überprüfung eines Sicherheitsabdruckes, gemäß der im Oberbegriff der Ansprüche 1 und 8 bzw. 10 angegebenen Art.

[0002] Ab einer mittleren bis höheren Anzahl an zu versendenden Briefen oder anderen Postgütern sind Frankiermaschinen zum Frankieren der Postgüter besonders effektiv einsetzbar. Im Unterschied zu anderen Druckgeräten eignet sich eine Frankiermaschine für die Bearbeitung von gefüllten Briefumschlägen, gegebenenfalls auch von sehr unterschiedlichem Format. Jedoch ist die Druckbreite auf die Breite des Frankierabdruckes begrenzt. Wenn nachfolgend zur Abkürzung das Wort Brief, Poststück oder Druckträger benutzt wird, schließt das natürlich alle Arten an Briefkuverts bzw. andere Aufzeichnungsträger mit ein. Als Aufzeichnungsträger können Postgut, Karteikarten, Etiketten oder selbstklebende Streifen aus Papier oder ähnlichem Material verwendet werden.

[0003] Moderne Frankiermaschinen setzen vollelektronische digitale Druckvorrichtungen ein. Beispielsweise weist die Frankiermaschine T1000 der Anmelderin ein Thermodruckwerk auf. Mit diesem ist es prinzipiell möglich, beliebige Texte und Sonderzeichen im Frankierstempeldruckbereich zu drucken. Die aus US 4.746.234 bekannte Termotransfer-Frankiermaschine hat einen Mikroprozessor und ist von einem gesicherten Gehäuse umgeben, welches eine Öffnung für die Zuführung eines Briefes aufweist. Ein mechanischer Briefsensor (Mikroschalter) übermittelt ein Druckanforderungssignal an den Mikroprozessor betreffend eine Information zur Position des Briefes bei dessen Zuführung. Der Mikroprozessor steuert dann die Antriebsmotore und einen Thermotransferdruckkopf. Ein Encoder übermittelt dabei ein aus dem Thermotransferfarbbandtransport abgeleitetes Signal an den Mikroprozessor als Information zur Brieftransportbewegung. Der Aufdruck des Frankierstempels erfolgt spaltenweise.

[0004] In der DE 196 05 014 C1 ist bereits eine Ausführung für eine Druckvorrichtung (JetMail®) vorgeschlagen worden, die bei einem nichtwaagerechten annähernd vertikalen Brieftransport einen Frankierdruck mittels einem hinter einer Führungsplatte in einer Ausnehmung stationär angeordneten Tintenstrahldruckkopf durchführt. Mit einem solchen ist ein vollelektronisches digitales Drucken sogar berührungslos möglich. Ein Drucksensor ist zur Briefanfangserkennung kurz vor der Ausnehmung für den Tintenstrahldruckkopf angeordnet und wirkt mit einem Inkrementalgeber zusammen. Durch die auf einem Transportband angeordnete Andruckelemente ist der Brieftransport schupffrei möglich.

[0005] Ein aus der US 4 949 381 bekanntes Sicherheitssystem verwendet Aufdrucke in Form von Bitmaps in einem gesonderten Markierungsfeld unter dem Frankiermaschinenstempeldruck. Obwohl die Bitmaps besonders dicht gepackt sind, wird durch die immer noch erforderliche Größe des Markierungsfeldes das Stempelbild in seiner Höhe um die Höhe des Markierungsfeldes verkleinert. Damit geht zuviel von der Druckfläche verloren, welche anderenfalls für Werbeklischeedaten oder andere Daten genutzt werden könnte. Ein hochauflösender Druckkopf ist natürlich relativ teuer. Nachteilig ist auch die zur Auswertung der Markierung erforderliche hochauflösende Erkennungseinrichtung.

[0006] Da die Darstellung eines eindimensionalen Bar- bzw. Strichcodes relativ viel Platz erfordern würde, ist auch schon ein ID-Matrix-Code vorgeschlagen worden. Ein anderer Vorschlag wurde in Technical Report Monograph 8, Symbol Technologies, April 1992 und in EP 439 682 B1 beschrieben und richtet sich auf eine PDF 417-Symbolik.

[0007] Die Postbestimmungen legen für Frankiermaschinen üblicherweise eine Breite des Frankierfeldes von einem Zoll (ca. 1 inch). Erste Abschätzungen ergeben für ein quadratisches Druckfeld mit einer Seitenlänge von einem inch eine Datenspeichermöglichkeit von maximal 400 bytes per square inch. Selbst wenn einerseits ein Druckkopf und andererseits ein Scanner mit entsprechender Auflösung entwickelt würden, wäre diese maximale Datenmenge im Abdruck in der Praxis für die Postbeförderung nicht erreichbar. Die Wahrscheinlichkeit von Abtastfehlern steigt mit der Anzahl an abgetasteten Daten. Bei höherer Druckauflösung kann eine Verschmutzung der Briefoberfläche bereits zu einem Fehler führen. Deshalb ist eine gewisse Redundanz der Daten von Vorteil, was ebenfalls die Anzahl an nutzbaren Bytes reduziert. Außerdem bleibt ein Nachteil zu beheben, daß jeder Barcode nur noch maschinell, d.h. nicht zusätzlich manuell überprüfbar ist. Folglich müßte zirca die halbe Druckbreite (1/2 inch) für die herkömmlichen visuell lesbaren Daten zur Verfügung gestellt werden. Wird dann die andere Hälfte für den maschinell lesbaren Code genutzt, können nicht alle Informationen, sondern beispielsweise mit der oben genannten JetMail® nur 30 byte, d.h. ca. 60 Digit sicher lesbar wiedergegeben werden. Bei niedriger Druckauflösung können Details weniger genau und somit eine geringere Anzahl an Digits dargestellt werden.

[0008] Die US-Post hat einen im Jahre 1996 veröffentlichten Forderungskatalog mit Anforderungen an die Konstruktion von zukünftigen sicheren Frankiermaschinen aufgestellt (Information based Indicia Program IBIP). Darin wird angeregt bestimmte Daten kryptografisch zu verschlüssen und in Form einer digitalen Unterschrift auf den zu frankierenden Brief zu drucken, anhand derer die US-Postbehörde Frankierabdrucke authentisieren kann. Bei der US-Postbehörde entsteht nach geschätzten Angaben durch Betrug ein jährlicher Schaden von ca. 200 Millionen US-$. Diese Anforderungen sind nach Art der Frankiereinrichtung differen-

ziert worden. Traditionelle Frankiermaschinen, welche in der Regel nur einen Frankierstempel (rot) aufdrucken werden auch als "closed systems" bezeichnet und brauchen (anders als bei sogenannten "open systems" (PC-Frankierer) die entsprechende Briefadresse nicht in die Verschlüsselung mit einbeziehen. Eine die Anschrift und einen Zahlencode (ZIP TO ZONE) umfassende Briefempfängeradresse (schwarz) kann bei der Brieferstellung durch einen üblichen Drucker auf das Kuvert aufgedruckt werden. Die als Zahlencode dargestellte Empfängeradresse wird erst in den Postzentren mit einem Optical Character Reader (OCR) abgetastet und für die Postverteilanlagen in maschinenlesbarer Form als Barcode (orange) auf den Briefumschlag aufgedruckt. Folglich besteht keine Bindung des Frankierabdruckes an eine bestimmte Briefempfängeradresse. Somit würde ein potentieller Fälscher, der auf der Frankiermaschinenseite nicht frankiert, sondern Farbkopien gleich schwerer Briefe erstellt, nur dann auf der Postseite, d.h. im Postamt auffallen, wenn alle Abdrucke gescannt und informationell in einer Datenbank gespeichert werden, wobei ein Vergleich mit allen gespeicherten Abdrucken die Einzigartigkeit des Frankierabdruckes beweisen muß, um als gültiges Orginal anerkannt zu werden. Der Aufwand auf der Postseite für eine komplette Archivierung aller Abdrucke und die Durchführung eines Vergleiches unter Echtzeitbedingungen wäre allerdings enorm. Wenn Prüfungen auf der Postseite aus Aufwandsgründen nur stichprobenartig möglich sind, verbleibt eine gewisse Wahrscheinlichkeit dafür, daß eine Fälschung unentdeckt bleibt.

[0009] In der EP 660 270 A2 wurden zur Sicherheit bereits zwei Maßnahmen , vorgeschlagen, nämlich ein Auswerteverfahren zur Ermittlung suspekter Frankiermaschinen in der Datenzentrale, welche die elektronische Guthabennachladung überwacht, und eine Überprüfung der Poststücke im Postamt oder in einem damit beauftragten Institut durchzuführen. Durch die Verwendung von Zeit/Datumsdaten als monoton stetig veränderbare Größe, kann wenigstens die Möglichkeit der Erstellung von unabgerechneten Farbkopien zeitlich begrenzt werden. Eine Frankiermaschine gilt als verdächtig, welche Auffälligkeiten im Verhalten bzw. Unregelmäßigkeiten zeigt, beispielsweise seit längerem keinen Kontakt zur Datenzentrale mehr hatte. Die Datenzentrale meldet suspekte Frankiermaschinen der Postbehörde, welche dann eine zielgerichtete Überprüfung der Poststücke vornimmt. Es wurde auch ein Verfahren und eine Anordnung zur Erzeugung und Überprüfung eines Sicherheitsabdruckes mit einer Markierungssymbolreihe vorgeschlagen. Die Graphik des Druckbildes kann durch Programmänderung der Frankiermaschine beliebig abgeändert werden. Neben den offen abgedruckten herkömmlichen visuell lesbaren Daten wird mit dem selben Druckkopf auch eine Markierungssymbolreihe gedruckt, damit das Druckbild einerseits vom Postbeamten manuell überprüft und andererseits auch maschinell ausgewertet werden kann. Das Druckbild ist nicht nur durch einfügbare Klischeetextteile bei Bedarf veränderbar, sondern die Markierung ändert sich aufgrund der monoton stetig veränderbaren Größe von Druck zu Druck, was ein derartig bedrucktes Poststück unverwechselbar macht. Alle wesentlichen Daten und die monoton stetig veränderbare Größe werden als eine Kombinationszahl zusammengestellt und dann verschlüsselt sowie anschließend in die vorgenannte Markierungssymbolreihe umgesetzt. Dadurch wird für eine solche Markierungssymbolreihe relativ wenig Platz gegenüber beispielsweise einem Barcode benötigt. In einer der zusätzlich angegebenen Auswertungsvarianten werden automatisch über ein geeignetes Lesegerät die Markierungen in einen Rechner eingegeben, der mit der Datenzentrale in Verbindung steht. Die Markierung wird in eine Kryptozahl zurückverwandelt. Separat dazu werden offen abgedruckte herkömmliche visuell (human) lesbare Daten mit einem OCR-Scanner abgetastet, um unter Verwendung einer Größe eine Vergleichskryptozahl zu bilden, wobei die Größe von der Datenzentrale dem Rechner auf der Postseite mitgeteilt wurde. Die Nachprüfung erfolgt im Rechner auf der Postseite durch Vergleich der vorgenannten Kryptozahl mit der vorgenannten Vergleichskryptozahl. Somit steht eine Zurückgewinnung von Frankierinformationen aus der Kryptozahl nicht mehr im Vordergrund und es ist hinreichend, wenn die Markierung eine Verifizierung der auf dem Poststück aufgedruckten Daten zuläßt. Bei einem solchen symmetrischen Verschlüsselungsverfahrens könnte aber prinzipiell die verschlüsselte Botschaft mit dem gleichen geheimen Schlüssel entschlüsselt werden, mit welchen sie verschlüsselt wurde.

[0010] In einer nicht vorveröffentlichten US-Anmeldung 08/798,604 mit dem Titel: "Methode and arrangement for generating and checking a security imprint" wurde bereits ein spezielles Secret Key Verfahren vorgeschlagen (Fig.1), für welches die vorgenannte Auswertevariante geignet ist, welche in EP 660 270 A2 zusätzlich erwähnt wurde. Der nachfolgend Secret Key genannte geheime Schlüssel wird in einer sicheren Datenbank an der Verifizierungsstelle, typischerweise bei der Postbehörde, aufgehoben und damit geheim gehalten. Aus der Botschaft wird ein Data Authentication Code (DAC) gebildet, was einer digitalen Unterschrift entspricht. Dabei wird der aus der US 3,962,539 bekannte Data Encryption Standard (DES)-Algorithmus angewendet, der in FIPS PUB 113 (Ferderal Information Processing Standards Publication) beschrieben wird. Die Symbole der Markierungssymbolreihe der digitalen Unterschrift sind in vorgenannter US-Anmeldung Ziffern, ggf. mit zusätzlichen Sonderzeichen. Die offen abgedruckten Informationen und die digitale Unterschrift im OCR-lesbaren Abschnitt des Druckbildes sind damit visuell (human) und maschinenlesbar.

[0011] Der bekannteste asymmetrische Kryptoalgorithmus ist der RSA-Algorithmus, nach US 4,405,829, der nach den Namen seiner Erfinder R.Rivest,

A.Shamir und L.Adleman benannt wurde. Bekanntlich entschlüsselt der Empfänger mit einem geheimen Schlüssel eine verschlüsselte Nachricht, welche beim Sender mit einem öffentlichen Schlüssel verschlüsselt wurde. RSA war das erste asymmetrische Verfahren, das sich auch zur Erstellung digitaler Unterschriften eignete. Aber RSA, wie auch andere digitale Signatur-Algorithmen (DSA) benutzen zwei Schlüssel, wobei einer der beiden Schlüssel öffentlich ist. Die Implementation des RSA-Algorithmus in einem Computer ergibt aber eine außerordentlich langsame Abarbeitung und liefert eine lange Signatur. Wegen der Länge der erzeugten digitalen Unterschrift würde auch beim Einsatz einer entsprechenden Symbolik (ID-Matrix, PDF 417 u.a.) ein übergroßer Abdruck erzeugt werden, den digital druckende Frankiermaschinen mit einem üblichen Druckkopf nicht liefern können.

[0012] Es wurde schon ein Digital Signatur Standard (DSS) entwickelt, der eine kürzere digitale Unterschrift liefert und zu dem der Digital Signatur Algorithm (DSA) nach US 5,231,668 gehört. Diese Entwicklung erfolgte ausgehend von der Identifikation und Signatur gemäß dem Schnorr-Patent US 4,995,085 und ausgehend vom Schlüsseltausch nach Diffie-Hellman US 4.200.770 bzw. vom ElGamal-Verfahren (El Gamal, Taher, "A Public Key Cryptosystem and a Signatur Scheme Based on Diskrete Logarithms", IIII Transactions and Information Theory, vol. IT-31, No. 4, Jul. 1985). Der geheime private Schlüssel ist aber nur schwer vor Diebstahl aus einem Computer zu schützen.

[0013] Mit einem symmetrischen Kryptoalgorithmus lassen sich Message Authentifications Code (MAC) und mit einem asymmetrischen Kryptoalgorithmus lassen sich digitale Unterschriften zur Authentifikation erzeugen. Beim symmetrischen Kryptoalgorithmus steht dem Vorteil eines relativ kurzen MACs der Nachteil eines einzigen geheimen Schlüssel gegenüber. Beim asymmetrischen Kryptoalgorithmus steht dem Vorteil des Verwendens eines öffentlichen Schlüssels der Nachteil einer relativ langen digitalen Unterschrift gegenüber.

[0014] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren für eine digital druckende Frankiermaschine und zur Überprüfung eines Sicherheitsabdruckes zu schaffen, wobei bei Gewährleistung einer hohen Sicherheit gegenüber Manipulation und Fälschung öffentliche Schlüssel verwendet werden und die zu druckende Informationsmenge soweit reduziert ist, daß für den Abdruck ein Druckkopf für eine bei Frankierungen üblichen Druckbreite eingesetzt werden kann. Der Abdruck soll außerdem in einem Teilabschnitt sicher maschinenlesbar sein.

[0015] Die Aufgabe wird mit den Merkmalen der Ansprüche 1, 8 und 10 gelöst.

[0016] Die für das erfindungsgemäße Verfahren unbedingt nötigen Frankierinformationen sind eine maschinenspezifische Kennung, eine monoton stetig veränderbare Größe und der Frankierwert.

[0017] Die Kennung, die mindestens den Absender anhand seiner Maschinenseriennummer identifiziert, ist frankiermaschinenintern gespeichert. Die frankiermaschinenintern erzeugte monoton stetig veränderbare Größe (Zeit oder incrementierte Stückzahl oder andere Größe) garantiert die Einzigartigkeit jedes Abdruckes. Der Frankierwert kann manuell eingegeben werden oder aufgrund einer Gewichtseingabe berechnet werden oder wird beispielsweise von einer Portorechnerwaage zur Frankiermaschine übermittelt. Diese vorgenannten unbedingt nötigen Frankierinformationen werden in einem ersten Abschnitt visuell vom Menschen lesbar und außerdem in einem zweiten Abschnitt unverschlüsselt als maschinenlesbarer Code aufgedruckt. Die konkreten Anforderungen für die aufzudruckenden Frankierinformationen werden von den Postbehörden bzw. von privaten Postbeförderern vorgegeben. Einerseits waren das Sicherheitsbedürfnis der Postbehörden zu berücksichtigen, andererseits werden in Frankiermaschinen nur die unbedingt nötigen Frankierinformationen in geeigneter Art und Weise zu einer digitalen Unterschrift verarbeitet, welche eine Verifizierung der Frankierabdrucke gestattet. Die digitale Unterschrift besteht aus einer verschlüsselten Botschaft, welche Bestandteil des Codes ist, der maschinenlesbar im zweiten Abschnitt aufgedruckt wird. Die Botschaft wird mindestens aus den unbedingt nötigen Frankierinformationen abgeleitet, welche maschinenlesbar unverschlüsselt aufgedruckt sind. Die ursprünglichen Daten werden ggf. einer Datenreduktion der Datenlänge auf eine vorbestimmte Länge unterworfen. Nach der Reduktion der Datenlänge auf eine Botschaft mit vorbestimmter Länge, können zwar die ursprünglichen Daten aus der digitalen Unterschrift nicht wieder zurückgewonnen werden, allerdings ist beim Einsatz einer Authentifikation die Fälschungssicherheit der im vorgenannten zweiten Abschnitt unverschlüsselt als maschinenlesbarer Code aufgedruckten unbedingt nötigen Frankierinformationen weiterhin gegeben.

[0018] Erfindungsgemäß sind folgende Verfahrensschritte vorgesehen:

- daß ein asymmetrisches Schlüsselpaar generiert wird, umfassend einen geheimen Schreibschlüssel Kw und einen öffentlichen Leseschlüssel Kr, wobei der geheime Schreibschlüssel Kw und ein asymmetrischer Verschlüsselungs-Algorithmus auf der Frankiermaschinenseite in einem postalischem Sicherheitsgerät (PSD) gespeichert ist, und wobei der zugehörige öffentliche Leseschlüssel Kr und sein Zertifikat der Frankiermaschinen-Kennung zugeordnet in einer Datenbank auf der Postbeförderseite gespeichert wird,
- daß die zu druckende maschinenlesbare Informationsmenge eine digitale Signatur und unverschlüsselte wesentliche Frankierinformationen enthält, wobei die unverschlüsselten wesentlichen Frankierinformationen mindestens eine Frankiermaschinen-Kennung, den Frankierwert und eine monoton

stetig veränderbare Größe enthalten, welche in eine Botschaft eingehen, und

- daß die Botschaft auf der Fankiermaschinenseite ggf. durch Reduktion vorgenannter wesentlicher Frankierinformationen gebildet und dann asymmetrisch mit dem geheimen Schreibschlüssel Kw verschlüsselt wird, vor einem Aufbereiten der Daten und Erzeugen der Drucksteuersignale zum Drukken.

[0019] Dabei wird ein modifiziertes Public Key Verfahren zum Erzeugen der verschlüsselten Botschaft in der Frankiermaschine in Form eines Programmes installiert, bei dem möglichst wenig Informationen auf den Brief maschinenlesbar aufgedruckt werden. Der Gedanke ist dabei, den privaten Schlüssel zuerst anzuwenden, um die Botschaft zu verschlüsseln. Der private Schlüssel wird nachfolgend Schreibschlüssel genannt. Die verschüsselte Botschaft kann mit dem öffentlichen Schlüssel wieder entschlüsselt werden. Dabei braucht der öffentlichen Schlüssel nicht mit auf dem Brief aufgedruckt zu werden. Der öffentlichen Schlüssel wird nachfolgend Leseschlüssel genannt. In einer gegenüber dem Secret Key Verfahren vorteilhaften Weise müssen nun in einer Datenbank keine geheimen sondern nur öffentliche Schlüssel verwaltet werden. Ein sogenannter Leseschlüssel und sein Zertifikat werden in der Datenbank der Postbehörde aufgehoben. Diese Datenbank muß nicht kryptographisch sicher sein, da sie ja allenfalls nur öffentliche Schlüssel enthält. Die Kennung der Frankiermaschine, die ja sowieso auf jedem Brief stehen muß, deutet auf ein Datenelement im Datenfile der Datenbank der Postbehörde, in welchem der Schlüssel mit seinem Zertifikat steht. Hierbei sind neben dem Zertifikat gegebenenfalls weitere übliche Maßnahmen vorgesehen, durch welche ein Einschleusen eines falschen Schlüssels in diese Datenbank ausgeschlossen ist. Insofern muß die Datenbank nur noch einer geringeren Sicherheitsanforderung genügen, welche schon heute Standard bei üblichen Computersystemen ist. Zusätzliche Sicherheitsmaßnahmen, welche beim Verwalten geheimer Schlüssel nötig wären, können entfallen.

[0020] Zur Überprüfung des Sicherheitsabdruckes auf der Postbeförderseite sind folgende Schritte vorgesehen:

- daß auf der Postbeförderseite aus den gescannten unverschlüsselten wesentlichen Frankierinformationen die Frankiermaschinen-Kennung abgetrennt und in eine Datenbank eingegeben wird, wobei in der Datenbank ein gespeicherter öffentlicher Leseschlüssel Kr und sein Zertifikat der Frankiermaschinen-Kennung zugeordnet ist,
- daß die Gültigkeit des Leseschlüssels Kr anhand seines Zertifikates überprüft und daß dann zur asymmetrischen Entschlüsselung der in der Datenbank gespeicherte öffentliche Leseschlüssel Kr verwendet wird, sowie
- daß eine Verifikation einerseits auf der Basis einer durch die asymmetrische Entschlüsselung gebildeten Botschaft und andererseits auf der Basis einer durch Reduktion der gescannten unverschlüsselten wesentlichen Frankierinformationen gebildeten Botschaft durchgeführt wird.

[0021] Für den Verifizierungsprozess kann dann die bei den Postbehörden vorliegende Datenbank einfach mitbenutzt werden, um die Aufdrucke aller Frankiermaschinen auf Einzigartigkeit zu überprüfen. Das gilt unabhängig vom konkret verwendeten Kryptoalgorithmus, welcher zwischen dem Frankiermaschinenhersteller und der Postbehörde vereinbart wurde. Im vorgenannten Datenfile existiert ein weiteres Datenelement, um die Art des verwendeten Kryptoalgorithmus zu speichern. Beim Verifizierungsprozess holt sich der Rechner der Auswerteeinrichtung der Postbehörde nun den richtigen Leseschlüssel aus der Datenbank, entschlüsselt die digitale Unterschrift zu einer Botschaft und führt dann die Verifikation auf Basis dieser Botschaft durch. Dazu wird aus den ebenfalls abgetasteten als maschinenlesbarer Code abgedruckten unverschlüsselten Informationen, wie Kennung, Stückzähler und Frankierwert eine Vergleichsbotschaft gebildet. Bei der Bildung der Botschaft in der Frankiermaschine vor dem Aufdrucken, wie bei der Bildung der Vergleichsbotschaft in der Auswerteeinrichtung nach dem Abtasten, wird der gleiche Algorithmus angewandt. Die Botschaft kann dann über einen geeigneten asymmetrischen Kryptoalgorithmus verschlüsselt werden.

[0022] In einer besonders vorteilhaften Variante des Verfahrens wird ein spezieller asymmetrischer Kryptoalgorithmus eingesetzt, der eine wesentlich kürzere digitale Unterschrift erzeugt, als beispielsweise RSA bzw. Digital Signatur Standard (DSS).

[0023] Dabei werden zugleich die vorgenannten Probleme im Zusammenhang mit dem Sicherheitsabdruck gelöst, welche bei Frankiermaschinen, die Druckköpfe mit weniger großer Druckauflösung verwenden oder welche bei der Überprüfung des Sicherheitsabdruckes bei der Postbehörde auftreten.

[0024] Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren naher dargestellt. Es zeigen:

Figur 1, Flußplan des für einen maschinenlesbaren Code modifizierten alternativen Secret Key-Verfahrens.

Figur 2, Flußplan des für einen maschinenlesbaren Code erfindungsgemäß modifizierten Public Key-Verfahrens,

Figur 3a, 3b, Frankierabdruckbeispiele für PDF 417

unter Anwendung von RSA bzw. des Elliptic Curve Algorithmus ECA,

Figur 4, Details der erfindungsgemäß arbeitenden Druckeinrichtung der Frankiermaschine,

Figur 5, Blockschaltbild zur Ansteuerung der erfindungsgemäß arbeitenden Druckeinrichtung,

[0025] In der Figur 1 wird der Flußplan des Secret Key-Verfahrens dargestellt, welches weiterhin die Geheimhaltung des Schlüssels verlangt.

[0026] Entgegen der Tendenz weitere Daten in die Verschlüsselung einzubeziehen, wirken die begrenzte Druckfläche und erreichbare Auflösung limitierend. So wäre es schon aus Platzgründen nicht ohne weiteres möglich, bereits durch Austausch der Markierungssymbol- bzw. Ziffernreihe gegen den geforderten PDF 417-Code die IBIP-Anforderungen zu erfüllen. Da aus der verschlüsselten Botschaft nicht mehr die ursprünglichen Frankierinformationen abgeleitet werden muß, kann die Botschaft jedoch noch weiter bis zu einem Digit zusammengestrichen werden (Truncation). Damit reduziert sich die Anzahl der zu druckenden Informationen auf die offen abgedruckten Informationen und die digitale Unterschrift, welche nun ebenfalls als PDF 417-Symbolik maschinenlesbar abgedruckt werden können. Die offen abgedruckten Informationen sind dann mindestens Kennung, Stückzähler und Frankierwert. Die Kennung umfaßt die Identifikationsnummern des Herstellers und des Gerätes (Maschinenseriennummer). Allerdings wäre der Schlüssel auch bei einem derart modifizierten Secret Key Verfahren geheim zu halten, was hohe Sicherheitsanforderungen an die Datenbank und deren Verwaltung stellt.

[0027] In einem ersten Schritt 101 werden die unbedingt nötigen Frankierinformationen bereitgestellt, vorzugsweise Kennung, Stückzahl und der Frankierwert. Im zweiten Schritt 102 wird mit dem Geheimschlüssel Kw eine DES-Verschlüsselung zu einer verschlüsselten Frankierinformation vorgenommen. Dabei oder anschließend im dritten Schritt 103 erfolgt eine Trunkation zu einem Daten-Authentisierungs-Code DAC. Im vierten Schritt 104 werden die unverschlüsselten unbedingt nötigen Frankierinformationen zusammen mit dem DAC gemäß der gewählten Symbolik (zum Beispiel PDF 417) codiert und dann im folgenden fünften Schritt 105 beim Frankieren zusammen mit den visuell (human) lesbaren Daten auf ein Poststück aufgedruckt. Nach Beförderung des Briefes zum Beförderer wird in einem sechsten Schritt 106 der maschinenlesbare Abschnitt des Frankierabdruckes gescannt anschließend erfolgt eine Decodierung der gescannten Symbolik des Abdruckes. Die Frankierinformationen (Kennung, Stückzahl, Frankierwert) und der Daten-Authentisierungs-Code (DAC) liegen dann in einer entsprechenden Form vor, welche der Computer auf der Postseite weiterverarbeiten kann. Im siebenten Schritt 107 wird aus der Kennung ein Eintrag in einer kryptographisch sicheren Datenbank gesucht, welche den Geheimschlüssel Kw enthält. Im achten Schritt 108 werden mit dem Geheimschlüssel Kw eine DES-Verschlüsselung der unbedingt nötigen Frankierinformationen und dabei oder in einem anschließenden neunten Schritt 109 eine Trunkation zu einem Referenz-Daten-Authentisierungs-Code DAC' vorgenommen. Im zehnten Schritt 110 wird der im sechsten Schritt 106 aus dem gescannten und decodierten PDF 417-Abdruck zurückgewonnene Daten-Authentisierungs-Code DAC mit dem im achten bis neunten Schritt 108, 109 ermittelten Referenz-Daten-Authentisierungs-Code DAC' verglichen. Aus der Gleichheit wird auf die Gültigkeit, d.h. auf einen ordnungsgemäß abgerechneten Frankierwert geschlossen. Als DES-Verschlüsselung von längeren Datensätzen zu Frankierinformationen kann beispielsweise auch der bekannte Cipher Block Chaining mode (CBC) eingesetzt werden.

[0028] Die Figur 2 zeigt den Flußplan des erfindungsgemäß modifizierten Public Key-Verfahrens. In einem ersten Schritt 201 werden die unbedingt nötigen Frankierinformationen als Datensatz m bereitgestellt, vorzugsweise Kennung, Stückzahl und der Frankierwert. Im zweiten Schritt 202 wird auf dem Wege einer Datenreduktion eine Botschaft erzeugt. Hierbei kann eine Hash-Funktion H(m) eingesetzt werden. Im dritten Schritt 203 wird mit dem privaten Schreibschlüssel Kw eine Verschlüsselung zu einer verschlüsselten Botschaft encr.H(m) vorgenommen. Im vierten Schritt 204 werden die unverschlüsselten unbedingt nötigen Frankierinformationen zusammen mit der verschlüsselten Botschaft encr. H(m) in einen Code (zum Beispiel PDF 417) umgewandelt, der beim Frankieren im fünften Schritt 205 zusammen mit den visuell (human) lesbaren Daten auf ein Poststück aufgedruckt wird. Im fünften Schritt 205 erfolgt eine Erzeugung des Druckbildes mit elektronischen Einbetten der variablen Daten vor dem Frankieren. Nach Postabgabe bzw. Posteingang beim Postbeförderer wird in einem sechsten Schritt 206 der maschinenlesbare Abschnitt des Frankierabdruckes gescannt und dann anschließend eine Codewandlung vom maschinenlesbaren Code (PDF 417) zum unverschlüsselten Datensatz m' und zur verschlüsselten Botschaft encr.H(m) vorgenommen, welche die Echtheit des gescannten unverschlüsselten Datensatzes m' nachweisen soll. Im siebenten Schritt 207 wird aus der gescannten Kennung ein Eintrag in einer postalischen Datenbank gesucht, welcher den öffentlichen Leseschlüssel Kr enthält. Im achten Schritt 208 wird auf der Postseite analog dem zweiten Schritt 202 auf der Frankiermaschinenseite eine Datenreduktion des Datensatzes m' zu einer Botschaft H(m') durchgeführt, wobei sich der Datensatz m' aus den gescannten Daten ergibt. Im neunten Schritt 209 wird mit dem Leseschlüssel Kr eine Entschlüsselung der verschlüsselten Bot-

schaft encr.H(m) zum Orginal-Datensatz m vorgenommen. Im zehnten Schritt 210 wird die im sechsten Schritt 206 gescannte Unterschrift, die zur verschlüsselten Botschaft encr.H(M) zurückverwandelt und dann zur Botschaft H(m) entschlüsselt wurde, mit der im achten Schritt 208 ermittelten Botschaft H(M') verglichen. Aus der Gleichheit wird auf die Gültigkeit, d.h. auf einen ordnungsgemäß abgerechneten Frankierwert geschlossen. Bei Ungleichheit wird eine Fäl-schung vermutet. Zur asymmetrischen Verschlüsselung wird ein spezieller Algorithmus bevorzugt, welcher eine relativ kurze Signatur liefert.

[0029] Bei Anwendung eines Public Key oder asymmetrischen Verfahrens existieren zwei nicht gleiche Schlüssel als ein Schlüsselpaar: Der Schreibschlüssel Kw und der Leseschlüssel Kr. Es ist vorgesehen, daß der Schreibschlüssel Kw geheim und der Leseschlüssel Kr öffentlich ist. Um zu vermeiden, daß jemand unbefugt ein Kw/Kr-Schlüsselpaar erzeugt, werden die Leseschlüssel Kr mit einem von der Post vergebenen Zertifikat versehen. Dadurch kann die Post prüfen, ob der in der Datenbank aufgefundene Leseschlüssel Kr echt ist. Der zentrale Unterschied zum symmetrischen Sekret Key Verfahren ist hier,

1. der nicht geheime Leseschlüssel Kr wird zusammen mit dem Zertifikat in der Datenbank gespeichert und
2. die digitale Unterschrift encr.H(m) ist nicht abgekürzt, da sie in einem späteren Schritt ja wieder dekryptifiziert werden muß, um die Botschaft H(m) zurückzugewinnen, mit welcher der Vergleich bei der Verifikation durchgeführt wird.

[0030] Die ursprünglichen Daten betreffend die unbedingt nötigen Frankierinformationen werden mit einer HASH-Funktion H zu einer Botschaft H(m) reduziert, das heißt auf einen binären String mit einheitlich fester Länge, beispielsweise 64 bit gebracht. Alternativ zu solcher HASH-Funktion könnte auch eine Prüfsumme verwendet werden. Es wird also kein Geheimschlüssel benötigt. Solche HASH-Funktionen sind unidirectionale eindeutige Funktionen und nicht zu verwechseln mit ähnlichen Funktionen, welche einen Geheimschlüssel einsetzen, wie beispielsweise Message Authentication Codes (MACs), Cipher Block Chaining mode (CBC) oder ähnliche.

[0031] Die Botschaft kann dann über einen geeigneten speziellen asymmetrischen Kryptoalgorithmus verschlüsselt werden, der eine relativ kurze digitale Unterschrift erzeugt. In vorteilhafter Weise wird das ELGamal-Verfahren (ELG) verwendet. Das ELGamal-Verfahren (ELG) beruht auf der Schwierigkeit diskrete Logarithmen, d.h. den Wert x zu berechnen, wenn bei bekannter Basis g eine Primzahl p Modul ist und wenn (p-1)/2 ebenfalls eine Primzahl ist. In der mathematischen Formel:

$$y = g^x \bmod p \quad (1)$$

stehen drei Zahlen, d.h. der Rest y, die Basis g und der Modul p. welche den öffentlichen Schlüssel bilden. Der geheime Schlüssel x (mit $x < p$) ist der diskrete Logarithmus von y zur Basis g bezüglich des Modus p. Für die Schlüsselerzeugung wird eine N bit lange Primzahl gewählt. Beispielsweise ist N = 64 bit, dann wäre das eine 20 stellige Primzahl.

[0032] Der öffentliche Leseschlüssel Kr = f{y,g,p} wird zur Herstellernummer (Vendor-ID) und Maschinennummer (Device-ID) zugeordnet in einer Datenbank auf der Postseite zusammen mit einem Zertifikat gespeichert. Letzteres beweist die Echtheit des öffentlichen Leseschlüssels Kr. Ein Postage Security Device (PSD) auf der Frankiermaschinenseite liefert den geheimen Schreibschlüssel Kw und nimmt vorzugsweise auch die Verschlüsselung mit dem geeigneten speziellen asymmetrischen Kryptoalgorithmus vor.

[0033] Da die entstehende digitale Unterschrift etwa doppelt so lang ist, wie der Klartext m, wird letzterer einer Reduction unterworfen, indem beispielsweise einfach die Quersumme vom Klartext gebildet wird, welche ggf. einer Trunkation unterworfen wird. Alternativ sind auch andere geeignete H-Funktionen einsetzbar. Nach der Bildung eines Datensatzes H(m) wird ein geheimer Wert $k < p$ gebildet, wobei k zu p-1 teilerfremd ist. Für den Datensatzes H(m) werden die beiden Zahlen a und b berechnet:

$$a = g^k \bmod p \quad (2)$$

und

$$b = y^k \, m \bmod p \quad (3)$$

[0034] Der Mikroprozessor oder ASIC des PSD ist so programmiert, daß der geheime Wert k dann gelöscht wird. Die beiden Zahlen a und b bilden zwei verschlüsselte Blöcke A und B mit jeweils der Länge N = 64 bit, d.h. die digitale Unterschrift encr.H(m) ist in der Summe = 16 byte lang.

[0035] Der Klartext m ist 18 Digit (Vendor ID = 1 Digit, Device-ID = 7 Digit, Postatge amount = 5 Digit, Piece count = 5 Digit) lang, wobei jedes Digit mit 4 bit dargestellt werden kann. Damit ergeben sich 9 byte maschinenlesbarer Text. Zusammen mit der digitalen Unterschrift ergeben sich minimal 25 byte, welche sich mit PDF 417 und Fehlerkorrekturlevel von 2 bequem in bereits in einem maschinenlesbaren Bereich von ca. 60mm * 10mm darstellen lassen. Selbst eine Primzahl von doppelter Bitlänge ergibt noch einen in o.g. Bereich passenden maschinenlesbaren Text, vorrausgesetzt die Auflösung beim Drucken und Scannen ist ausreichend hoch.

[0036] Die auf den Brief gedruckte digitale Unterschrift und die unverschlüsselte maschinenlesbaren Daten werden gescannt und durch Decodierung in eine

digital binäre oder hexadezimale Form umgewandelt, welche sich leicht im Auswertegerät weiter verarbeiten läßt.

[0037] Zur Entschlüsselung wird die abgetrennte digitale Unterschrift encr.H(m) in zwei N-bi-Blöcke zerlegt. Für zwei aufeinander folgende Blöcke A, B wird die Gleichung (4) nach m' mit dem verallgemeinerten Euklidischen Algorithmus aufgelöst:

$$a^x m' = b \bmod p \quad (4)$$

[0038] Es gilt:

$$a^x m' = g^{kx} m' = g^{xk} m' = y^k m' = b \bmod p \quad (5)$$

Da gilt:

$$y^k m = b \bmod p \quad (6)$$

kann durch Vergleich der Werte aus den Gleichungen (5) und (6) auf die Gleichheit von m = m' geschlossen werden.

[0039] Alternativ kann auch ein anderer geeigneter Krypto-Algorithmus verwendet werden, wenn dies die Auflösung des Druckbildes zuläßt. Beispielsweise kann auch ein Elliptic Curve Algorithmus (ECA) verwendet werden. Seit Mitte der 80er Jahre, in welchem zuerst von Victor Miller (Miller, Victor: Use of Elliptic Curves in Cryptology; in Williams, H.C.(Hrsg.): Proceedings of Crypto '85, LNCS 218, Springer, Berlin 1986, S.417-426) und unabhängig auch von Neal Koblitz (Koblitz, Neal: Elliptic Curve Cryptosystems; Mathematics of Computation, Vol.48, No. 177, Jan. 1987, S.203-209) Elliptic Curve Cryptosysteme vorgeschlagen wurden, welche aber damals noch nicht praktikabel waren, wurde die Praktikabilität von Elliptic Curve Cryptosystemen verbessert. Ein 160 bit-Schlüssel eines Elliptic Curve Cryptosystems liefert inzwischen ein gleiches Sicherheitsniveau, wie ein 1024 bit-Schlüssel eines digitalen Signatursystems, wie beispielsweise RSA, welches auf der Komplexität des Faktorisierungsproblems beruht. Auch ein an ELGamal angelehntes Elliptic Curve Signatur Schema (ECSS) ist im Standard IEEE P1363 beschrieben. Dieses kann mit erheblich kürzeren Schlüsseln arbeiten als beispielsweise ein System allein basierend auf dem ELGamal-Verfahren. Der Rechenaufwand zur Erzeugung einer Signatur nach einem an ELGamal angelehnten Elliptic Curve Signatur Schema (ECSS) ist besonders geringer als bei Anlehnung an das RSA-Verfahren. Der Effizienzvorteil für auf Elliptischen Kurven basierende Signatursysteme nimmt für größere Schlüssellängen deutlich zu, da für die Lösung des Diskreten Logarithmusproblems auf Elliptischen Kurven bis heute kein subexponentieller Algorithmus bekannt ist.

[0040] Die Botschaft kann ebenso über einen anderen geeigneten speziellen asymmetrischen Kryptoalgorithmus verschlüsselt werden, der andere geeignete mathematische Formeln für ein auf Elliptischen Kurven basierendes Signatursystem benutzt.

[0041] Die damit erreichbare drastische Reduktion der zu druckenden Information im Vergleich zum normalen asymmerischen Public Key Verfahren gestattet sogar die Verwendung des PDF417-Codes, um mindestens die digitale Unterschrift sicher maschinenlesbar aufzudrucken. Das gemeinsame Aufdrucken der offen abgedruckten Informationen und der digitalen Unterschrift kann mit einem Druckkopf in der für Frankiermaschinen üblichen Druckbreite erfolgen.

[0042] Es ist aus der Figur 3a klar ersichtlich, daß der durch Anwendung des RSA-Verfahrens signierte Frankierabdruck eine größere Druckbreite erfordert, als bei Anwendung des erfindungsgemäßen Verfahrens.

[0043] Die Figur 3b zeigt einen gemäß dem erfindungsgemäß modifizierten Public Key-Verfahren erzeugten Frankierabdruck. Im Vergleich mit dem - in Fig. 3a gezeigten - unter Anwendung des RSA-Verfahrens signierten Frankierabdruckes kann die Druckbreite geringer sein. Über dem maschinenlesbaren Bereich ist der visuell (human) lesbare Bereich und ein Bereich für den FIM-Code gemäß den Postvorschriften angeordnet. Links davon liegt ein weiterer Druckbereich, welcher vorzugsweise zum Drucken eines Werbeklischees verwendet werden kann. Wegen des FIM-Code ergibt sich ein ca 11 bis 14 mm breiter visuell (human) lesbarer Bereich. Somit kann die restliche Breite für den maschinenlesbaren Bereich verwendet werden. Aufgrund der Datenbank, welche die Leseschlüssel mit zugehörigem Zertifikat verwaltet, müssen letztere nicht im maschinenlesbaren Bereich des Abdruckes mit abgedruckt sein.

[0044] Natürlich kann alternativ mit dem modifizierten Sekret Key-Verfahren ein ähnlich aussehender Frankierabdruck erzeugt werden, wie er in Fig. 3b gezeigt ist. Die Fälschungssicherheit ist jedoch stark von der Truncation abhängig und nicht so hoch wie beim erfindungsgemäß modifizierten Public Key-Verfahren. Aus dem Vergleich der beiden Figuren 1 und 2 ergibt sich klar der Vorteil des erfindungsgemäß modifizierten Public Key-Verfahrens nach Fig.2, weil der gegen Angriffe zu verteidigende Bereich (starke schwarze Umrandung) hier kleiner ist und beispielsweise als schnelle Hardware-Schaltung (ASIC) ausgeführt werden kann, welche gegen Angriffe sicherer als eine reine Software-Lösung ist.

[0045] Die Datenbank, welche die Leseschlüssel verwaltet, muß nicht zusätzlich gegen das elektronische Ausspähen dieser Schlüssel gesichert sein. Dadurch ist es möglich eine verteilte Datenbank zu verwenden, d.h. weitgehend lokale Datenbanken mit den für die gemeldeten Frankiermaschinen Schlüsseln, wobei die Datenbanken untereinander Daten austauschen können.

[0046] Die Figur 4 zeigt Details der erfindungsgemäß arbeitenden Druckeinrichtung zum Bedrucken eines auf einer Kante 31 stehenden Briefkuvertes 3. Diese besteht im wesentlichen aus einem Transportband 10,

einer orthogonal zur Transportebene (XZ-Ebene) und einer über dieser in der XY-Ebene angeordneten Führungsplatte 2 sowie einem Tintendruckkopf 4. Das Briefkuvert 3 ist so gewendet und gedreht daß es mit seiner Oberfläche an den Führungschienen 23 der Führungsplatte 2 anliegt. Die Führungsplatte 2 ist vorzugsweise in einem Winkel $\gamma = 18°$ zum Lot geneigt. Führungsplatte 2 und Transportband 10 bilden miteinander einen Winkel von 90°. Die auf dem Transportband 10 stehenden Briefkuverte 3 liegen zwangsläufig an der Führungsplatte 2 durch die Schräglage derselben an und werden außerdem durch Andruckelemente 12 angedrückt, welche auf dem Transportband 10 befestigt sind. Bei Bewegung des Transportbandes 10 gleiten die Briefe 3 mitgenommen durch die Andruckelemente 12 an den Führungsschienen 23 der feststehenden Führungsplatte 2 entlang. Ein Fortsatz 12132 der Anruckelemente 12 gleitet dabei auf einer Kulisse mit den Auslenkungen 81 bzw. 82, welche das Andrücken bzw. Freigeben des Briefkuvertes vor bzw. nach dem Drukken ermöglicht. In der Führungsplatte 2 ist eine Ausnehmung 21 für den Tintendruckkopf 4 vorgesehen. Die Führungsplatte 2 ist in Transportrichtung stromabwärts im Bereich 25 hinter den Ausnehmungen 21 gegenüber der Anlagefläche für den Brief 3 so weit zurückversetzt, daß die bedruckte Fläche mit Sicherheit frei liegt. Die in der Führungsplatte 2 angeordneten Sensoren 17 bzw. 7 dienen zur Vorbereitung bzw. Briefanfangserkennung und Druckauslösung in Transportrichtung. Die Transporteinrichtung besteht aus einem Transportband 10 und zwei Walzen 11 Eine der Walzen 11 ist die mit einem Motor 15 ausgestattete Antriebswalze. Beide Walzen 11 sind vorzugsweise in nicht dargestellter Weise als Zahnwalzen ausgeführt, entsprechend auch das Transportband 10 als Zahnriemen, was die eindeutige Kraftübertragung sichert. Ein Encoder 5, 6 ist mit der Antriebswalze 11 gekoppelt. Vorzugsweise sitzt die Antriebswalze 11 mit einem Inkrementalgeber 5 fest auf einer Achse, gleichfalls nicht sichtbar. Der Inkrementalgeber 5 ist beispielsweise als Schlitzscheibe ausgeführt, die mit einer Lichtschranke 6 zusammen wirkt.

[0047] Die Figur 5 zeigt ein Blockschaltbild zur Ansteuerung der Druckvorrichtung 20 mit einer Steuereinrichtung 1. Die Steuereinrichtung 1 umfaßt ein Meter mit einem postalischen Sicherheitsgerät PSD 90 mit einem Datumsschaltkreis 95, mit einer Tastatur 88 und mit einer Anzeigeeinheit 89 sowie einen anwendungsspezifischen Schaltkreis ASIC. Das postalische Sicherheitsgerät PSD 90 besteht aus einem Mikroprozessor 91 und an sich bekannten Speichermitteln 92, 93, 94, die zusammen in einem gesicherten Gehäuse untergebracht sind. Der Programmspeicher ROM 92 enthält auch einen Verschlüsselungsalgorithmus und den geheimen Schreibschlüssel Kw. Der Mikroprozessor 91 kann alternativ als OTP (one Time Programmable) ausgebildet sein, der das Programm für die Verschlüsselung und den geheimen Schreibschlüssel Kw speichert.

[0048] Das postalische Sicherheitsgerät PSD 90 kann auch eine Hardware-Abrechnungsschaltung enthalten. Eine solche kann prinzipiell Softwareaßnahmen manipuliert werden. Nähere Ausführungen finden sich beispielsweise in der europäischen Anmeldung EP 789 333 A2 mit dem Titel: Frankiermaschine.

[0049] Das postalische Sicherheitsgerät PSD 90 kann auch als Sicherheitsmodul SM speziell für einen Personalcomputer ausgebildet sein, welcher eine Frankiermaschinen-Basis steuert. Nähere Ausführungen dazu erfolgen in der nicht vorveröffentlichten deutschen Anmeldung 197 11 998.0, welche den Titel trägt: Postverarbeitungssystem mit einer über Personalcomputer gesteuerten druckenden Maschinen-Basisstation.

[0050] Der anwendungsspezifische Schaltkreis ASIC der Steuereinrichtung 1 weist eine Schnittstellenschaltung 97 auf und steht über letztere mit dem Mikroprozessor 91 in Kommunikationsverbindung. Das ASIC weist außerdem die zugehörige Schnittstellenschaltung 96 zu der in der Maschinenbasis befindlichen Schnittstellenschaltung 14 auf und stellt mindestens eine Verbindung zu den Sensoren 6, 7, 17 und zu den Aktoren, beispielsweise zum Antriebsmotor 15 für die Walze 11 und zu einer Reinigungs- und Dichtstation RDS für den Tintenstrahldruckkopf 4, sowie zum Tintenstrahldruckkopf 4 der Maschinenbasis her. Die prinzipielle Anordnung und das Zusammenspiel zwischen Tintenstrahldruckkopf und der RDS sind der nicht vorveröffentlichten deutschen Anmeldung 197 26 642.8 entnehmbar, mit dem Titel: Anordnung zur Positionierung eines Tintenstrahldruckkopfes und einer Reinigungs- und Dichtvorrichtung.

[0051] In vorteilhafter Weise ist der Drucksensor 7 als Durchlichtschranke ausgebildet. Beispielsweise ist eine Sendediode der Durchlichtschranke des Drucksensors 7 in der Führungsplatte 2 und im Abstand dazu, entsprechend der maximale Dicke (in Z-Richtung) der Poststücke (Briefe), eine Empfangsdiode der Durchlichtschranke angeordnet. Beispielsweise ist die Empfangsdiode an einem Trägerblech 8 an der Kulisse befestigt. Genauso wirksam wäre eine umgekehrte Anordnung mit Empfangsdiode in der Führungsplatte 2 und Sendediode am Trägerblech 8. Damit werden bei dünnen wie bei dicken Briefen auf immer gleiche Weise der Briefanfang (Kante) exakt detektiert. Der Drucksensor 7 liefert das Startsignal für die Wegsteuerung zwischen diesem Sensor 7 und der ersten Tintenstrahldruckkopfdüse. Die Drucksteuerung erfolgt auf Basis der Wegsteuerung, wobei der gewählte Stempelversatz berücksichtigt wird, welcher per Tastatur 88 eingegeben und im Speicher NVM 94 nichtflüchtig gespeichert wird. Ein geplanter Abdruck ergibt sich somit aus Stempelversatz (ohne Drucken), dem Frankierdruckbild und gegebenfalls weiteren Druckbildern für Werbeklischee, Versandtinformationen (Wahldrucke) und zusätzlichen editierbaren Mitteilungen.

[0052] Es ist vorgesehen, daß die einzelnen Druckelemente des Druckkopfes innerhalb seines Gehäuses mit einer Druckkopfelektronik verbunden sind und daß der

Druckkopf für einen rein elektronischen Druck ansteuerbar ist. Der Encoder 5, 6 liefert pro n Druckspalten ein Signal an den Microprozessor. Dies geschieht per Interruptfunktion. Bei jedem Interrupt wird auch ein Bandzähler aktualisiert, der den Bewegungsfortschritt des Motors 15 und somit des Transportbandes 10 festhält. Jede Druckspalte ist vorzugsweise 132 µm breit. Der Bandzähler ist hierbei ein Zweibyte-Zähler, d.h. 21^{16}-1 Zählerstände sind möglich. Hiermit kann also ein maximaler Briefverfahrweg von $W_{max} = 65535 * 132\mu m * n$ erfaßt werden.

[0053] Mit dem Vorbereitungssensor 17 wird eine Briefbewertungsroutine angestoßen. Der Vorbereitungssensor 17 detektiert die Briefvorderkante, was vom Mikroprozessor registriert wird, um den Bandzähler zu starten, der die Encoderimpulse aufsummiert, bis die Briefvorderkante den Drucksensor 7 erreicht. Die aufsummierte Impulszahl wird mit der dem Weg zwischen Vorbereitungssensor 17 und Drucksensor 7 entsprechenden Impulszahl verglichen. Die zulässige Abweichung für den ersten definierten Briefverfahrweg W_{def1} beträgt 10 %. Die Drucksteuerung bzw. Sensorabfragen sind also alle weggesteuert. Die Drucksteuerung erfolgt für einen spaltenweise gedruckten Abdruck, dessen Druckspalten einen vorbestimmten Winkel $10° \leq \alpha \leq 90°$ zur Transportrichtung einnehmen.

[0054] Die visuell und die maschinenlesbaren variablen Druckbilddaten werden in die übrigen fixen bzw. semivariablen Druckbilddaten elektronisch eingebettet und spaltenweise gedruckt. Ein geeignetes Verfahren ist beispielsweise der europäischen Anmeldung EP 762 334 A1 entnehmbar, welche den Titel trägt: Verfahren zum Erzeugen eines Druckbildes, welches in einer Frankiermaschine auf einen Träger gedruckt wird.

[0055] Die Figur 5 zeigt noch eine weitere Schnittstellenschaltung 99, welche nach rechts über ein Datenkabel 19 mit einer Schnittstellenschaltung 18 der poststromabwärts nachfolgenden Ablagestation verbunden ist und deren Steuerung durch die Steuereinrichtung 1 gestattet. Ein anderes Peripheriegerät links der die Steuereinrichtung 1 und Druckvorrichtung 20 umfassenden Frankiermaschinenbasis ist vorzugsweise eine automatische Zuführstation 28 und mit ihrer Schnittstellenschaltung 13 über Kabel 16 und mit einer Schnittstellenschaltung 98 des ASIC verbunden. Es ist vorgesehen, daß weitere Sensoren in den vorgenannten weiteren Stationen zur Detektierung der Briefkanten angeordnet sind, welche über vorgenannte Schnittstellen mit dem Mikroprozessor 91 in der Steuereinrichtung 1 gekoppelt sind, um den Systembetrieb zu ermöglichen bzw. zu überwachen.

[0056] Der nicht vorveröffentlichten deutschen Anmeldung 197 11 997.2 ist eine für die Peripherieschnittstelle geeignete Ausführungsvariante für mehrere Peripheriegeräte (Stationen) entnehmbar. Sie trägt den Titel: Anordnung zur Kommunikation zwischen einer Basisstation und weiteren Stationen einer Postbearbeitungsmaschine und zu deren Notabschaltung.

[0057] Die Steuereinrichtung und Druckvorrichtung kann auch unterschiedlich von der bisher beschriebenen Ausführungsform realisiert sein. Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die vom gleichen Grundgedanken der Erfindung ausgehend, die von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Verfahren für eine digital druckende Frankiermaschine zur Erzeugung eines Sicherheitsabdruckes, wobei wesentliche Frankierinformationen zusammen mit einer Signatur auf ein Poststück im maschinenlesbaren Bereich des Frankierbildes aufgedruckt werden, wobei eine digitale Druckvorrichtung (20) von einer Steuereinrichtung (1) gesteuert wird, die Drucksteuersignale für einen Druckkopf (4) üblicher Druckbreite erzeugt, um die Druckträgeroberfläche mit einem entsprechenden Druckbild zu bedrucken, während das Poststück (3) am Druckkopf (4) vorbei transportiert wird, **gekennzeichnet dadurch,**

   - daß ein asymmetrisches Schlüsselpaar generiert wird, umfassend einen geheimen Schreibschlüssel (Kw) und einen öffentlichen Leseschlüssel (Kr), wobei der geheime Schreibschlüssel (Kw) und ein asymmetrischer Verschlüsselungs-Algorithmus auf der Frankiermaschinenseite in einem postalischem Sicherheitsgerät (PSD) gespeichert ist, und daß der zugehörige öffentliche Leseschlüssel (Kr) und sein Zertifikat der Frankiermaschinen-Kennung zugeordnet in einer Datenbank auf der Postbefördererseite gespeichert wird,
   - daß die zu druckende maschinenlesbare Informationsmenge eine digitale Signatur und unverschlüsselte wesentliche Frankierinformationen enthält, wobei die unverschlüsselten wesentlichen Frankierinformationen mindestens, eine Frankiermaschinen-Kennung, den Frankierwert und eine monoton stetig veränderbare Größe enthalten, welche in eine Botschaft eingehen,
   - daß die Botschaft auf der Fankiermaschinenseite durch Reduktion vorgenannter wesentlicher Frankierinformationen gebildet und dann asymmetrisch mit dem geheimen Schreibschlüssel (Kw) verschlüsselt wird, vor einem Aufbereiten der Daten und Erzeugen der Drucksteuersignale zum Drucken.

2. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch,** daß das modifizierte Public Key-Verfahren einen speziellen Algorithmus zur asymmetri-

schen Ver/Entschlüsselung verwendet, der eine relativ kurze Signatur liefert.

3. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch,** daß das modifizierte Public Key-Verfahren auf einem modifizierten ELGamal-Verfahren basiert.

4. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch,** daß das modifizierte Public Key-Verfahren auf einem modifizierten elliptic curve Verfahren basiert.

5. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch,** daß die Reduktion durch Anwendung einer Hash-Funktion auf die vorgenannten wesentlichen Frankierinformationen erfolgt.

6. Verfahren, nach einem der vorgenannten Ansprüche 1 bis 5, **gekennzeichnet dadurch,** daß die maschinenlesbare Informationsmenge vor dem Drucken in einen maschinenlesbaren Code bzw. in eine Symbolik codiert wird.

7. Verfahren, nach Anspruch 6, **gekennzeichnet dadurch,** daß die Symbolik eine PDF 417-Symbolik ist.

8. Verfahren zur Überprüfung eines Sicherheitsabdruckes mit Transport des Poststückes zum Postbeförderer, mit Scannen der maschinenlesbaren Information und mit Entschlüsselung der Signatur zu einer Botschaft zu deren Verifikation auf der Postbeförderereseite,
gekennzeichnet dadurch,

   - daß auf der Postbeförderereseite aus den gescannten unverschlüsselten wesentlichen Frankierinformationen die Frankiermaschinen-Kennung abgetrennt und in eine Datenbank eingegeben wird, wobei in der Datenbank ein gespeicherter öffentlicher Leseschlüssel (Kr) und sein Zertifikat der Frankiermaschinen-Kennung zugeordnet ist,
   - daß die Gültigkeit des Leseschlüssels (Kr) anhand seines Zertifikates überprüft und daß dann zur asymmetrischen Entschlüsselung der in der Datenbank gespeicherte öffentliche Leseschlüssel (Kr) verwendet wird, sowie
   - daß eine Verifikation einerseits auf der Basis einer durch die asymmetrische Entschlüsselung gebildeten Botschaft und andererseits auf der Basis einer durch Reduktion der gescannten unverschlüsselten wesentlichen Frankierinformationen gebildeten Botschaft durchgeführt wird.

9. Verfahren, nach Anspruch 8, **gekennzeichnet dadurch,**
daß die gescannte Signatur ein Matrixcode ist, der vor der Entschlüsselung decodiert wird und daß die vorgenannte Reduktion durch Anwendung einer Hash-Funktion auf die vorgenannten wesentlichen Frankierinformationen erfolgt.

10. Verfahren für eine digital druckende Frankiermaschine zur Erzeugung und Überprüfung eines Sicherheitsabdruckes mit folgenden Schritten:

   - Bereitstellung der unbedingt nötigen Frankierinformationen als Datensatz m im ersten Schritt 201,
   - Erzeugung einer Botschaft H(m) auf dem Wege einer Datenreduktion im zweiten Schritt 202,
   - asymmetrische Verschlüsselung zu einer verschlüsselten Botschaft encr.H(m) mit dem privaten Schreibschlüssel Kw im dritten Schritt 203,
   - Umwandlung der unverschlüsselten unbedingt nötigen Frankierinformationen zusammen mit der verschlüsselten Botschaft encr.H(m) in einen Matrixcode im vierten Schritt 204,
   - Erzeugung des Druckbildes mit elektronischen Einbetten der variablen Daten und Frankieren im fünften Schritt 205, wobei die maschinenlesbaren Daten zusammen mit den human lesbaren Daten auf ein Poststück aufgedruckt vom selben Druckkopf aufgedruckt werden,
   - Postabgabe des Poststückes an den Postbeförderer und Scannen des Poststückes beim Postbeförderer in einem sechsten Schritt 206, wobei der maschinenlesbare Abschnitt des Frankierabdruckes gescannt und dann anschließend eine Codewandlung vom Matrixcode zum unverschlüsselten Datensatz m' und zur verschlüsselten Botschaft encr.H(m) vorgenommen wird, welche die Echtheit des gescannten unverschlüsselten Datensatzes m' nachweisen kann,
   - Suchen eines Eintrages in einer postalischen Datenbank im siebenten Schritt 207, wobei aufgrund der gescannten Kennung gesucht wird und wobei der Eintrag den öffentlichen Leseschlüssel Kr enthält,
   - Datenreduktion des Datensatzes m' zu einer Botschaft H(m') im achten Schritt 208 auf der Postbeförderereseite,
   - Entschlüsselung der verschlüsselten Botschaft encr.H(m) zum Orginal-Datensatz m im neunten Schritt 209, wobei der Leseschlüssel Kr verwendet wird,
   - Vergleich im zehnten Schritt 210, der im sechsten Schritt 206 gescannten Unterschrift, die zur verschlüsselten Botschaft encr.H(M) zurückverwandelt und dann zur Botschaft H(m)

entschlüsselt wurde, mit der im achten Schritt 208 ermittelten Botschaft H(M'), wobei aus der Gleichheit auf die Gültigkeit, d.h. auf einen ordnungsgemäß abgerechneten Frankierwert geschlossen wird.

11. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch,**

    - daß die als Datensatz m bereitgestellten unbedingt nötigen Frankierinformationen, vorzugsweise Kennung, Stückzahl und der Frankierwert umfassen.

12. Verfahren, nach Anspruch 1, **gekennzeichnet dadurch,**

    - daß zur asymmetrischen Ver/Entschlüsselung ein spezieller Algorithmus eingesetzt wird, welcher eine relativ kurze Signatur liefert und daß der maschinenlesbare Code eine PDF 417-Symbolik ist.

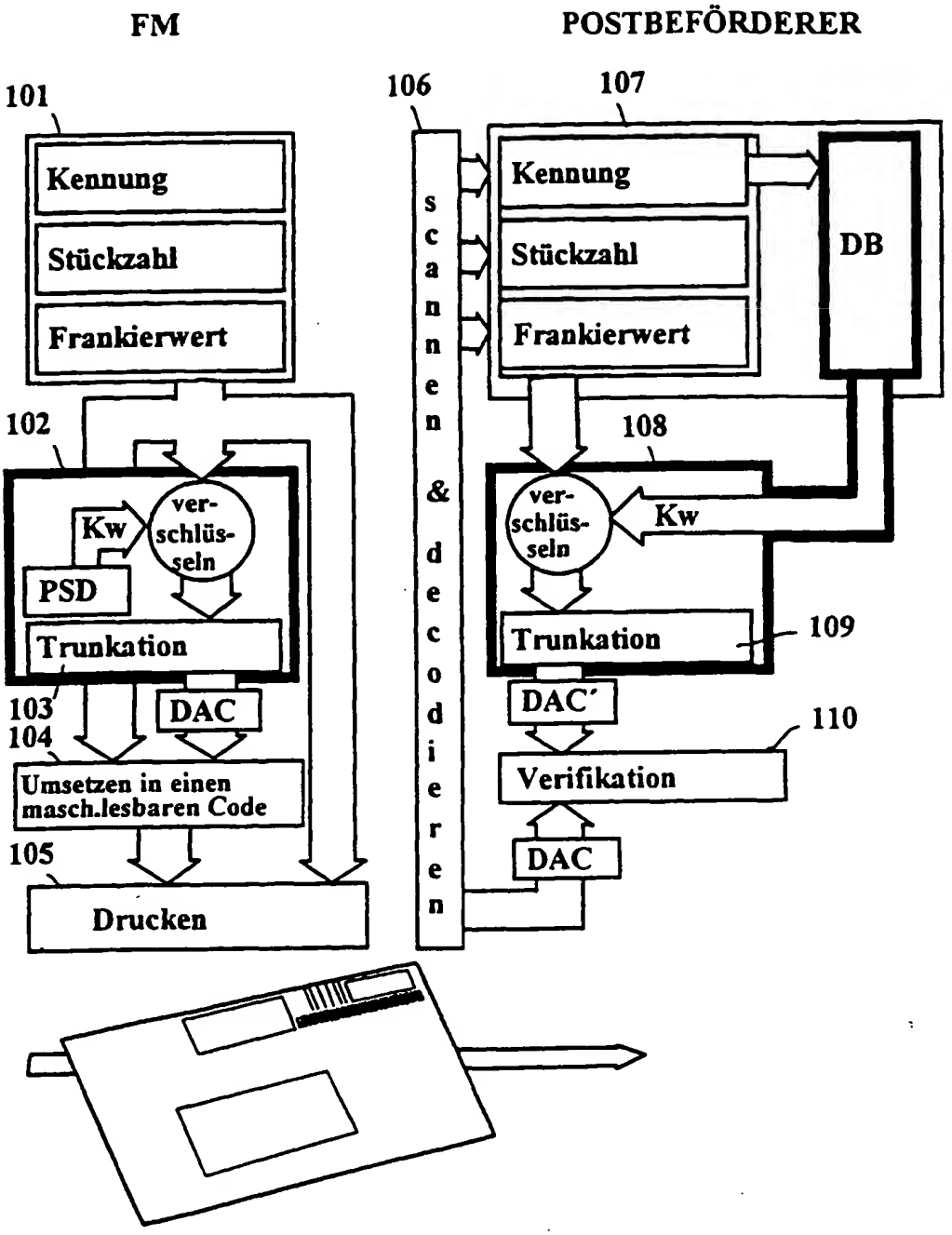
FM
POSTBEFÖRDERER
101
Kennung
Stückzahl
Frankierwert
102
Kw
ver-
schlüs-
seln
PSD
Trunkation
103
104
DAC
Umsetzen in einen
masch.lesbaren Code
105
Drucken
106
scannen & decodieren
107
Kennung
Stückzahl
Frankierwert
DB
108
ver-
schlüs-
seln
Kw
Trunkation
109
DAC'
110
Verifikation
DAC

Fig. 1

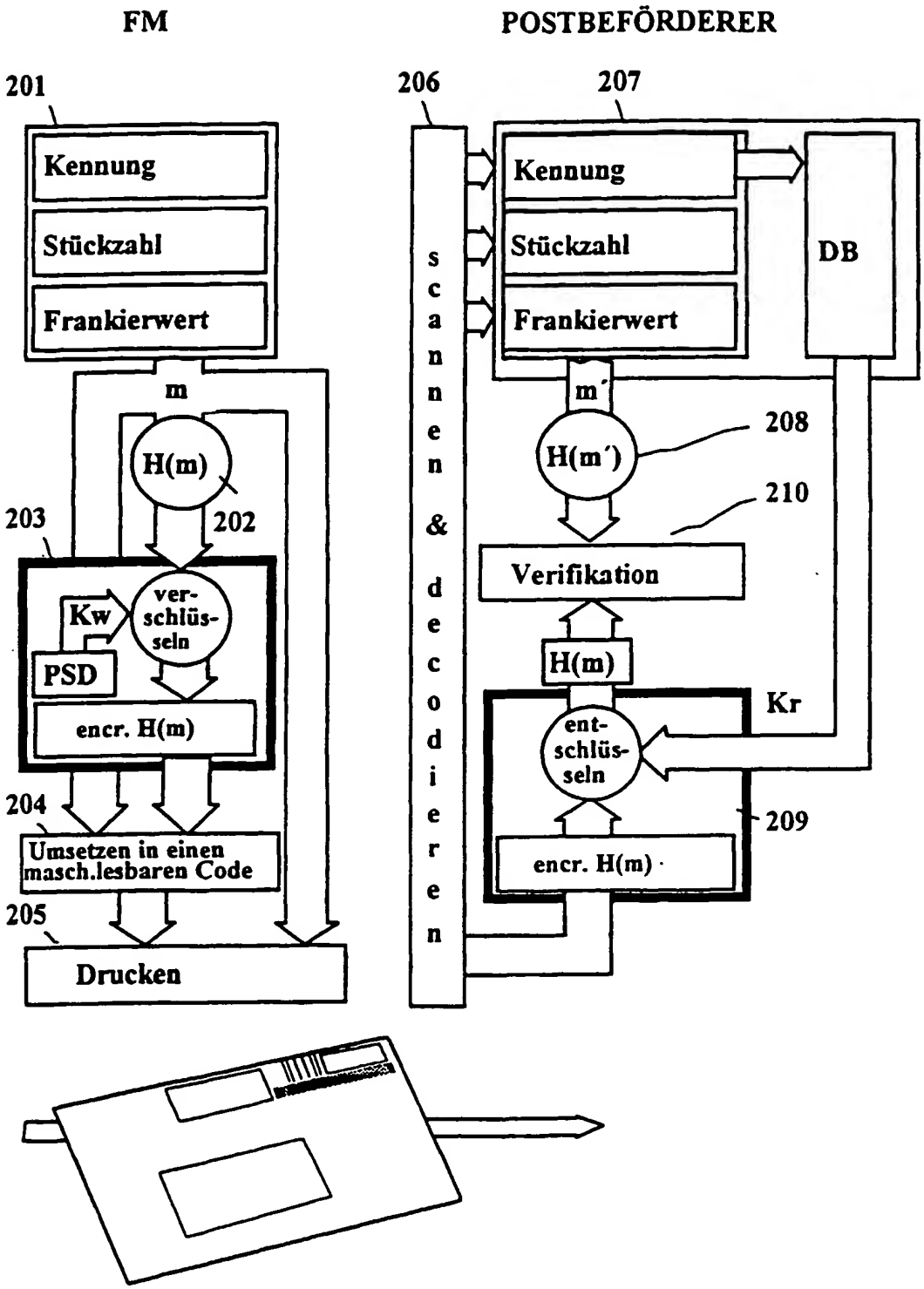
FM
POSTBEFÖRDERER
201
206
207
Kennung
Stückzahl
Frankierwert
DB
scannen & decodieren
m
m'
H(m)
H(m')
208
210
202
203
Kw
ver-
schlüs-
seln
PSD
encr. H(m)
Verifikation
H(m)
Kr
ent-
schlüs-
seln
209
encr. H(m)
204
Umsetzen in einen
masch.lesbaren Code
205
Drucken

Fig. 2

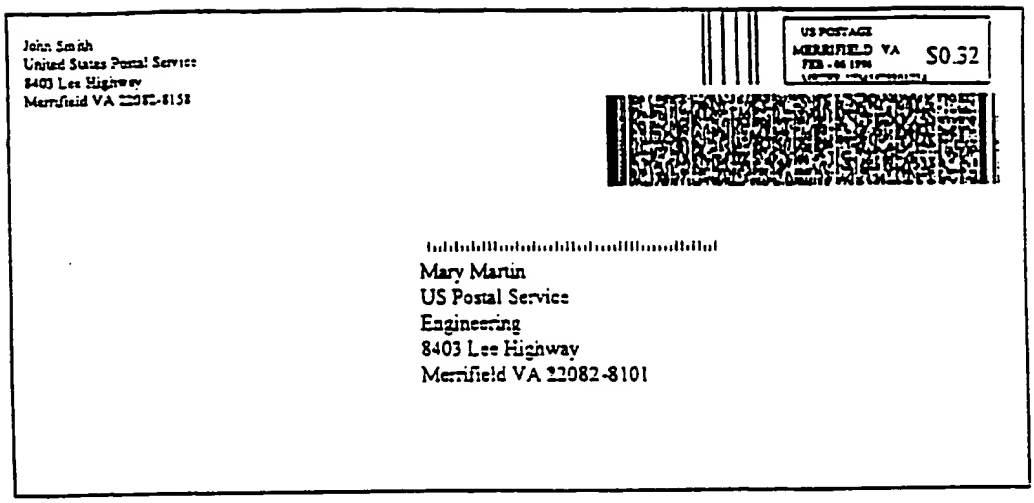
John Smith
United States Postal Service
8403 Lee Highway
Merrifield VA
US POSTAGE
MERRIFIELD VA
$0.32
Mary Martin
US Postal Service
Engineering
8403 Lee Highway
Merrifield VA 22082-8101

Fig. 3a

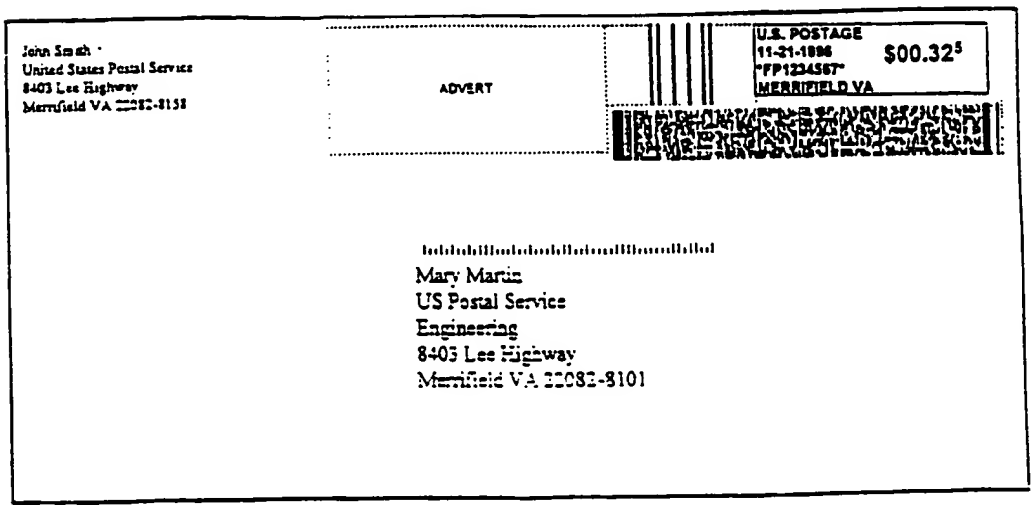
John Smith
United States Postal Service
8403 Lee Highway
Merrifield VA
ADVERT
U.S. POSTAGE
11-21-1996
"FP1234567"
MERRIFIELD VA
$00.32⁵
Mary Martin
US Postal Service
Engineering
8403 Lee Highway
Merrifield VA 22082-8101

Fig. 3b

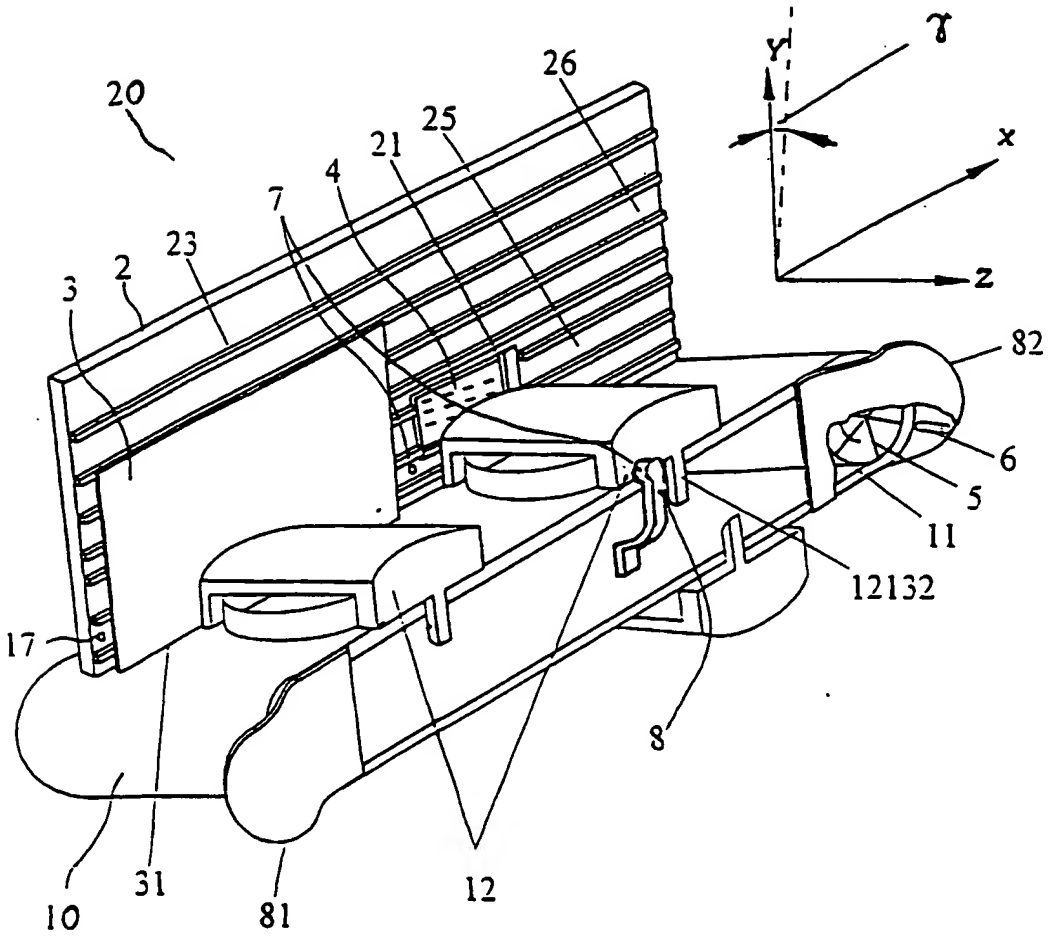

Fig. 4

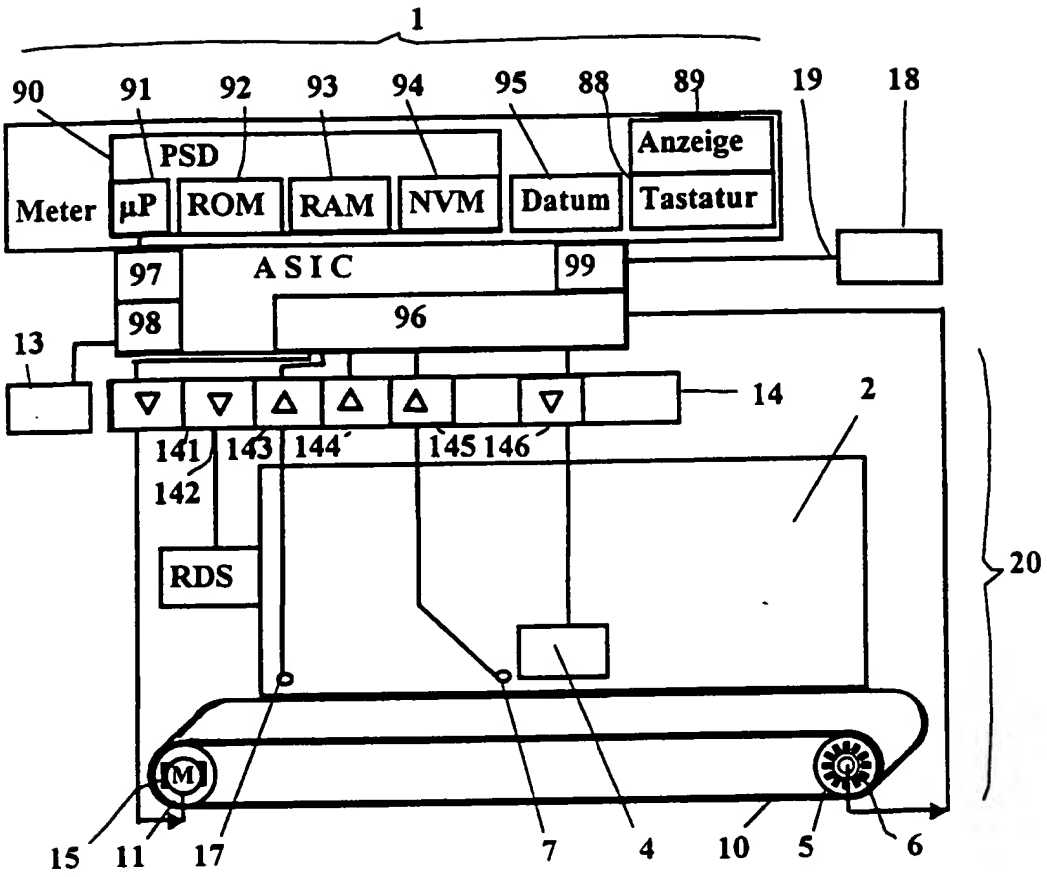
1
90
91
92
93
94
95
88
89
19
18
PSD
Meter
µP
ROM
RAM
NVM
Datum
Anzeige
Tastatur
97
ASIC
99
98
96
13
14
2
141
143
144
145
146
142
RDS
20
M
15
11
17
7
4
10
5
6

Fig. 5